UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

RAFAEL HERNANDEZ, individually and on behalf of all others similarly situated, Plaintiff, v. FLAGSTAR BANCOPR, INC., and FLAGSTAR BANK, FSB, Defendants.	Civil Action No.: 2:22-CV-11887 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Rafael Hernandez ("Plaintiff"), on behalf of himself and all others similarly situated, by and through his undersigned counsel, brings this action against Flagstar Bancorp, Inc. and Flagstar FSB (collectively "Flagstar" or "Defendant"). Plaintiff alleges as follows upon personal knowledge as to the facts pertaining to himself, and on information and belief as to all other matters.

I. SUMMARY OF THE ACTION

1. Flagstar Bancorp, Inc., a publicly traded company headquartered in Troy, Michigan, is a savings and loan holding company that owns and operates Flagstar Bank, FSB. Through Flagstar Bank, FSB, Defendant provides commercial, business, and personal banking services in several states and offers mortgage loans throughout the United States.

2. On June 17, 2022, Flagstar disclosed, for the first time, a cyber-attack that occurred between December 3 and 4, 2021 in which unauthorized individuals accessed the personal identifiable information ("PII") of approximately 1,547,169 consumers (the "Data Breach"). The hackers who undertook the data breach accessed critical PII including, at the very least, names and Social Security Numbers. Defendant has failed to disclose when it learned of the Data Breach and has failed to explain why it took more than six months for Flagstar to begin notifying affected consumers.

3. Plaintiff brings this action on behalf of himself and the class of consumers defined herein (the "Class"), the members of which (the "Class Members") had their PII, including but not limited to, names and Social Security numbers disclosed to unauthorized third persons as a result of the Data Breach.

4. Defendant is a financial institution that provides banking and mortgage services to consumers. As a condition of receiving banking and/or mortgage services from Defendant, consumers provide their PII to Defendant.

5. Plaintiff and Class Members entrusted this sensitive confidential information to Defendant. This information was compromised and unlawfully accessed due to the Data Breach. The information remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons, and is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' PII.

7. The Data Breach occurred because Defendant maintained Class Members' PII in a reckless manner and on its computer networks in a condition that was vulnerable to cyber-attacks. The risk of cyber-attack was well-known to Defendant – and to all financial service companies – and Defendant was continuously on notice at all times material that its failure to take steps necessary to secure the PII from a risk of cyber-attack and unauthorized access left that information and property in a dangerous condition that was vulnerable to theft.

8. Defendant's failure to protect the PII of consumers is all the more egregious because, not only was Defendant aware of the significant risk of cyber-attacks faced by financial institutions given the sensitive nature of the PII entrusted to them, but Defendant was exposed to another data breach early in 2021, when a file sharing platform operated by one of Defendant's vendors was accessed in an unauthorized data breach.

9. Nevertheless, and despite this knowledge and recent exposure to a data breach, Defendant continuously disregarded the rights of Plaintiff and Class Members, as more fully defined below, by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its data systems were protected and safeguarded against unauthorized intrusions, while failing to disclose that it did not have adequately robust computer systems and security safeguards or practices in place with respect to protecting against the risk of unauthorized access of PII. Defendant further failed to take standard and reasonably available steps to prevent the Data Breach, and failed to properly train its staff and employees on proper security measures. Importantly, Defendant also failed to provide Plaintiff and Class Members with prompt and timely notice of the Data Breach, thereby further injuring them by such delay.

10. Defendant and its employees failed to properly monitor the computer networking systems on which it housed the PII and, had they done so, would have discovered the intrusion sooner, and would not have permitted cyber thieves to freely access Flagstar's IT network for a substantial period of time.

11. Plaintiff's and Class Members' identities are now at risk as a consequence of Defendant's misconduct. Their PII that was collected by the Defendant and maintained at all times material, without adequate safeguards, is now in the hands of cyber thieves – a present risk that will continue throughout their respective lifetimes.

12. Defendant was fully aware that data thieves, once armed with PII that they accessed in a data breach, are capable of pursuing numerous types of misconduct and crimes through the unauthorized use and exploitation of that data, including opening new financial accounts in Class Member's names, taking loans in their names, using their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

13. Plaintiff and Class Members have suffered numerous actual and imminent injuries as a direct result of the Data Breach, including: (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of the Data Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damages to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their PII against theft and not allow access to and misuse of their personal data by others; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further injurious breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff and Class Members' PII, and, at the very least, are entitled to nominal damages.

14. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals who are Class Members, and further seeks remedies that include, but are not limited to, compensatory damages, nominal damages and reimbursement of out-of-pocket costs, as well as injunctive and equitable relief to prevent future injury on behalf of himself and the putative class.

II. PARTIES

Plaintiff

15. Plaintiff Hernandez is, and at all times mentioned herein was, a resident of the state of Florida, residing in the City of Miami. Plaintiff obtained a mortgage through Flagstar Bank, FSB. Plaintiff provided PII, including his name and Social Security Number, as well as additional information, to Flagstar

Bank FSB. Plaintiff was only recently notified of the Data Breach and that his PII was compromised upon receiving the Notice of the Data Breach.

Defendant

16. Defendant Flagstar Bancorp, Inc., a savings and loan holding company, is publicly traded on the New York Stock Exchange under the FBC ticker symbol and is headquartered in Troy, Michigan.

17. Flagstar Bank, FSB, is a wholly-owned subsidiary of Flagstar Bancorp, Inc. and provides commercial, small business, and consumer banking services through 158 branches located in Michigan, Indiana, California, Wisconsin, and Ohio. Flagstar FSB also provides home loans to consumers throughout the United States and operates 84 retail loan center locations in 28 states. Flagstar Bank FSB is a federally chartered stock savings bank and maintains its headquarters in Troy, Michigan.

III. JURISDICTION AND VENUE

18. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, are citizens of states different than that of Defendant.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant is authorized to conduct business within this District, is headquartered in this District, has intentionally availed itself of the laws in this District, and conducts substantial business, including acts underlying the allegations of this complaint, in this District.

IV. FACTUAL ALLEGATIONS

Flagstar and Its Business

20. Flagstar Bancorp, Inc., a savings and loan holding company, is publicly traded on the New York Stock Exchange under the FBC ticker symbol and is headquartered in Troy, Michigan. Flagstar Bank, FSB, is a wholly-owned subsidiary of Flagstar Bancorp, Inc. and provides commercial, small business, and consumer banking services through 158 branches located in Michigan, Indiana, California, Wisconsin, and

Ohio. Flagstar FSB also provides home loans to consumers throughout the United States and operates 84 retail loan center locations in 28 states.

21. Flagstar collected, stored, and maintained the PHI provided by Plaintiff and Class Members as a condition of providing services. Such PHI included names and Social Security numbers.

22. In order to apply for a mortgage, refinance a mortgage, or obtain other financial services from Flagstar, Plaintiff and Class Members were required to and did in fact turn over such PII to Defendant.

23. Defendant maintains a privacy policy (the "Privacy Policy") that provides notice of its privacy practices (the "Privacy Notice") with respect to how it handles customer PII.[1] In the Privacy Notice, Flagstar assures consumers that "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[2]

24. Defendant was aware at all times material of the fact that the financial industry was at risk of experiencing a cyber-security attack and data breach as many have occurred throughout the United States. Given its maintenance of critical PII and its knowledge of such risk and its duties, Defendant was responsible for safeguarding the PII in its possession with respect to each Plaintiff and Class Member.

The Cyber-Attack and Data Breach

25. On June 17, 2022, Flagstar began informing affected customers that, between December 3 and December 4, 2021, Flagstar's network systems were accessed by an unauthorized individual or individuals.[3] Flagstar indicated that it concluded its investigation of the Data Breach on June 2, 2022.[4]

26. In its notice to affected individuals, Flagstar asserted that:

> Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and

[1] https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf, last visited August 10, 2022.

[2] *Id.*

[3] *Id.*

[4] *Id.*

> reported the matter to federal law enforcement. After an extensive forensic investigation and manual document review, we discovered on June 2, 2022 that certain impacted files containing your personal information were accessed and/or acquired from our network between December 3, 2021 and December 4, 2021.[5]

27. The Flagstar Notice failed to disclose when Flagstar learned of the attack. *Id.* However, despite Flagstar's assurance that it had exercised "an abundance of caution" in deciding to notify consumers whose PII had been accessed, Flagstar took more approximately six months from the date of the Data Breach to notify consumers of the Data Breach. Indeed, when Flagstar learned of the Data Breach, rather than alert customers it "engaged external cybersecurity professionals experienced in handling these types of incidents" and notified "federal law enforcement." *Id.* Thereafter, Flagstar remained silent for more than six months, when it began providing notice of the Data Breach to approximately 1.54 million customers.

28. Defendant provided notice to the Attorney General of Maine, indicating that it had begun providing notice to affected consumers on June 17, 2022.[6] In the notice to the Attorney General of Maine, Flagstar acknowledged that the "information acquired" in the Data Breach included, "[n]ame or other personal identifier in combination with: **Social Security Number**."[7] However, as of August 10, 2022, Defendant had yet to provide notice to the Attorney General of Texas, despite the fact that Flagstar maintains a loan center in Houston, Texas.[8, 9]

29. In its notice to consumers, Flagstar offered to provide just two years of credit monitoring and identity repair services to affected consumers, a woefully inadequate solution given the theft of valuable PII, including names and Social Security numbers which, when used in conjunction with each other, pose a lifetime risk of identity theft.

30. Plaintiff is informed and believes that the cyber-attack targeted Defendant by reason of its status as a financial institution that collects, creates, and maintains PII, and that such attack was designed

---

[5] June 17, 2022 Flagstar Bank Notification, attached hereto as Exhibit A.

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml, last visited on August 10, 2022.

[7] *Id.* (Emphasis in original).

[8] https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage, last visited on August 10, 2022.

[9] https://www.flagstar.com/branch-locator.html, last visited on August 10, 2022.

to gain access to and infiltrate private and confidential data, including the PII of Plaintiff and Class Members.

31. Defendant did not state in its Notice of the Data Breach why it was unable to detect the unauthorized individuals accessing Defendant's servers or why it had waited for more than six months before notifying affected patients and members.

32. The Data Breach occurred as a direct and proximate result of Defendant's failure to prevent the cyber-attack and as a consequence of the fact that it did not adhere to commonly accepted securities standards and otherwise failed to detect that its databases were subject to a security breach.

33. The significant risk of a cyber-attack and data breach was unquestionably foreseeable to Defendant.

34. The Data Breach could have been prevented had Defendant properly secured and encrypted Plaintiff's and Class Members' PII, destroyed data, including old data Defendant had no legal right or responsibility to retain.

35. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users, configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[10]

36. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[11]

---

[10] How to Protect Your Networks from Ransomware, available at https://www.justice.gov/criminal-ccips/file/872771/download (last visited August 10, 2022).

[11] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), available at: https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited August 10, 2022).

37. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates

- Use threat and vulnerability management

- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities

- Hunt for brute force attempts

- Monitor for cleanup of Event Logs

- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall

- Enable tamper protection

- Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[12]

[12] *See* Human-operated ransomware attacks: A preventable disaster - Microsoft Security Blog (last visited August 10, 2022); Microsoft Shares Tactics Used in Human-Operated Ransomware Attacks (bleepingcomputer.com) (last visited August 10, 2022).

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. Because Defendant was entrusted with consumers' PII, it had, and has, a duty to protect that PII and keep it secure.

40. Plaintiff and Class Members reasonably expect that when their PII is provided to Defendant, it will safeguard their PII.

41. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

42. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

43. Upon information and belief, the occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

44. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

45. Defendant's failure to keep secure current and former customers' PII has had and shall continue to have adverse effects that are long lasting and severe. Once Social Security numbers and other PII have been stolen, fraudulent use of that information and damage to victims may continue for years.

PII is Uniquely Valuable to Hackers

46. PII, including names and social security numbers are uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Member's names, take loans in their names, use their names to obtain medical services, obtain government benefits, file fraudulent

tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

47. Social Security numbers are among the most sensitive kind of personal information. They are difficult for an individual to change. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.[13]

48. A new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

49. For this reason, hackers prey on financial institutions and related entities. And financial institutions, like Defendant, have been aware of this, and the need to take adequate measures to secure their systems and information, for a number of years. In 2021 alone, approximately 279 breaches targeting financial service providers occurred.[15] That figure represented a substantial increase from the year before and the year before that.[16] The steady growth of hacks of financial services providers is no surprise and can be tied to two significant factors, (1) the failure of financial services providers, like Defendant, to adequately protect patient data and (2) the substantial value of the sensitive PII entrusted to financial service providers.

50. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high.[17] These data breaches exposed the sensitive data of approximately 294 million people. *Id.* Hackers are

---

13 Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions worrying-about-identity-theft (last accessed August 10, 2022)

14 *Id.*

15 ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) at 6. (last visited on August 10, 2022).

16 *Id*.

17 ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) (last visited on August 10, 2022).

increasingly targeting highly sensitive PII, including social security numbers and, in 2021, approximately 1,136 data breaches exposed social security numbers. *Id.*

51. Financial service providers like Flagstar are well aware of the risk that data breaches pose to consumers, especially because both the size of Flagstar's customer base and the fact that the PII that they collect and maintain from their customers is profoundly valuable to hackers. Indeed, Federal Reserve Chairman Jerome Powell has referred to cyber-attacks as the number one threat to the global financial system.[18]

Plaintiff's Experiences

52. Plaintiff typically takes measures to protect his PII and is very careful about sharing his PII. Plaintiff does not knowingly transmit unencrypted PII over the internet or other unsecured source.

53. Plaintiff Hernandez stores any documents containing his PII in a safe and secure location. He also diligently chooses unique usernames and passwords for his online accounts.

54. As a result of the Data Breach, Plaintiff Hernandez has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors accounts and credit scores and has sustained emotional distress as a result of worrying about his PII being exfiltrated. He has monitored his account extensively since receiving the Notice of Data Breach from Defendant, and intends to spend time taking steps to protect his PII. This is time that was and will be lost and unproductive and taken away from other activities and duties.

55. Plaintiff Hernandez has suffered, and will continue to suffer, lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, emotional distress, and increased concerns for the loss of his privacy.

56. As a result of the Data Breach and the exfiltration of his unencrypted PII in the hands of criminals, Plaintiff Hernandez is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

[18] For Financial Institutions, Cyberthreats Loom Large (forbes.com) (last visited August 10, 2022).

57. To date, Defendant has done very little to adequately protect Plaintiff and Class Members, other than informing them of the availability of free credit reports and offering two years of credit monitoring and identify theft protection, and has done nothing to compensate them for their injuries sustained in this Data Breach.

Plaintiff's and Class Members' Damages

58. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security, or agent's data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of the breach.

59. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. This ongoing need for monitoring for identity theft and fraud will extend indefinitely into the future.

60. Consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen even absent any adverse use. When this type of sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Consumers must spend time and money to re-secure their financial position and safeguard their standing in the financial community.

61. Plaintiff and the other Class Members have suffered and will suffer actual injury due to loss of time and increased risk of identity theft as a direct result of the Data Breach. In addition to any fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiff and the other Class Members suffer ascertainable losses in the form of out-of-pocket expenses, opportunity costs, and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach.

62. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of their PII, including making sure that the storage of data or documents containing PII is not accessible by unauthorized persons and that access to such data is sufficiently protected.

63. In addition to the remedy for economic harm, Plaintiff and the Class Members maintain an undeniable and continuing interest in ensuring that the PII remains in the possession of Defendant is secure, remains secure, and is not subject to future theft.

V. CLASS ALLEGATIONS

64. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiff asserts common law claims on behalf of himself and all Class Members for negligence (Count I), breach of implied contract (Count II), and breach of fiduciary duty (Count III), on behalf of the Nationwide Class defined below and violation of the Florida Deceptive and Unfair Trade Practices Act (Count IV) on behalf of the Florida Class defined below:

Nationwide Class: All residents of the United States whose PII was accessed or otherwise compromised as a result of the Data Breach.

Florida Class: All residents of the state of Florida whose PII was accessed or otherwise compromised as a result of the Data Breach

Members of the Nationwide Class and the Florida Class are referred to herein collectively as "Class Members" or "Class."

65. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

66. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

67. **Numerosity**: The exact number of members of the Class is unknown to Plaintiff at this time but, on June 17, 2022, Defendant acknowledged in a notice provided to the Attorney General of Maine that

the number of "persons affected" by the Data Breach was 1,547,169, indicating that there are more than 1.5 million members of the Nationwide Class, making joinder of each individual impracticable.[19] There are hundreds of thousands of members of the Class, making joinder of each individual impracticable. Ultimately, members of the Class will be easily identified through Defendant' records.

68. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

b) Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

c) Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members, respectively, to unauthorized third parties;

d) Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

e) Whether and when Defendant learned of the Data Breach;

f) Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g) Whether Defendant committed violations by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h) Whether Defendant failed to implement and maintain reasonable security procedures and practices adequate to protect the information compromised in the Data Breach, considering its nature and scope;

i) Whether Defendant has adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j) Whether Defendant engaged in unfair, unlawful, or deceptive practices, including by failing to safeguard the PII of Plaintiff and Class Members;

[19] https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml (last visited on August 10, 2022).

k) Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct, and if so, in what amount;

l) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct, and if so, in what amount; and

m) Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

69. **Typicality**: Plaintiff's claims are typical of the claims of the members of the Class. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

70. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

71. **Risks of Prosecuting Separate Actions**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, Defendand still collects and maintains the PII of Plaintiff, the Class and other consumers in the course of its business and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PII entrusted to Defendant.

72. **Policies Generally Applicable to the Class**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

73. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

74. **Manageability**: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

75. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

76. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

77. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

VI. CAUSES OF ACTION

Negligence
(On Behalf of Plaintiff and the Nationwide Class)

78. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 77.

79. As a condition of receiving their mortgages or other financial services from Defendant, Defendant's current and former customers were obligated to provide and entrust Defendant with certain PII, including their name, Social Security number, and other PII and financial information in connection with a loan application, loan modification, other items regarding loan servicing, or other financial services.

80. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

81. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

82. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

83. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

84. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

85. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII, and to employ proper procedures to prevent the unauthorized

dissemination of the PII of Plaintiff and the Class.

86. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

87. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

88. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

89. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

90. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

91. Plaintiff and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

92. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

93. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

94. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by

unauthorized third persons as a result of the Data Breach.

95. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

96. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

97. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former customers' PII in the face of increased risk of theft.

98. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

99. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

100. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

101. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

102. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class' PII was accessed and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

103. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

104. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's

conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

105. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

106. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

107. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

108. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former customers' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

109. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

110. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which

remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

111. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is now at an increased risk of identity theft or fraud.

112. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

113. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 77.

114. Defendant acquired and maintained the PII of Plaintiff and the Class, including name, Social Security number, and other PII, including their name, Social Security number, and other PII and financial information in connection with a loan application, loan modification, other items regarding loan servicing, or other financial services.

115. At the time Defendant acquired the PII of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

116. Plaintiff and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements such as Social Security numbers, and not delete the PII that Defendant no longer had a reasonable need to maintain.

117. Prior to the Data Breach, Defendant published the Privacy Policy, agreeing to protect and keep private financial information of Plaintiff and the Class.

118. Defendant further promised to protect Plaintiff's and Class Members' PII through the use of computer safeguards and secured files and buildings.

119. Implicit in the agreement between Plaintiff and Class Members and the Defendant to

provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

120. In collecting and maintaining the PII of Plaintiff and the Class and publishing the Privacy Policy, Defendant entered into contracts with Plaintiff and the Class requiring Defendant to protect and keep secure the PII of Plaintiff and the Class.

121. Plaintiff and the Class fully performed their obligations under the contracts with Defendant.

122. Defendant breached the contracts they made with Plaintiff and the Class by failing to protect and keep private financial information of Plaintiff and the Class, including failing to (i) encrypt or tokenize the sensitive PII of Plaintiff and the Class, (ii) delete such PII that Defendant no longer had reason to maintain, (iii) eliminate the potential accessibility of the PII from the internet where such accessibility was not justified, and (iv) otherwise review and improve the security of the network system that contained such PII.

123. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

124. As a direct and proximate result of Defendant's breach of contract, Plaintiff is at an increased risk of identity theft or fraud.

125. As a direct and proximate result of Defendant's breach of contract, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class)

126. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 77.

127. A relationship existed between Plaintiff and the Class and Defendant in which Plaintiff and the Class put their trust in Defendant to protect the private information of Plaintiff and the Class. Defendant accepted that trust and the concomitant obligations.

128. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

129. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

130. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of its current and former customers' PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

131. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and the Class's information in Defendant's possession was adequately secured and protected.

132. Defendant also had a fiduciary duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant, and because Defendant was the only party in a position to know of its inadequate security measures and capable of taking steps to prevent

the Data Breach.

133. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class by failing to act with the utmost good faith, fairness, and honesty, failing to act with the highest and finest loyalty, and failing to protect the private information of Plaintiff and the Class.

134. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and the Class.

135. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred.

136. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and the Class.

137. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

COUNT IV
Violation of the Florida Deceptive and Unfair Trade Practices Act (Fla. Stat. §§ 501.201, *et seq.*
(On behalf of Plaintiff and the Florida Class)

138. Plaintiff and the Florida Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 77.

139. Defendant's conduct, as alleged in this complaint, included transactions involving trade and commerce. Specifically, Defendant obtained the PII of Plaintiff and the Florida Class by advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiff and the Florida Class and the Data Breach occurred through the use of an instrumentality of interstate commerce, the internet.

140. Defendant's conduct, as alleged herein, constituted unfair or deceptive acts or practices in the conduct of consumer transactions, including, inter alia:

a. failure to adequately protect and safeguard the PII of Plaintiff and the Florida Class;

b. failure to prevent unauthorized disclosure of the PII of Plaintiff and the Florida Class;

c. failure to disclose that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and the Florida Class from unauthorized exfiltration; and

d. failure to disclose the Data Breach to Plaintiff and the Florida Class in a timely and accurate manner.

141. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant's immoral, unethical, oppressive, and unscrupulous activities are and were substantially injurious to Plaintiff and the Florida Class.

142. In committing the acts alleged herein, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to Plaintiff and the Florida Class that it failed to adopt industry best practices in the collection, storage, use, and granting of access to the PII of Plaintiff and the Florida Class.

143. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff and the Florida Class are entitled to an order providing declaratory and injunctive relief and, to the extent allowed by law, Plaintiff and the Florida Class are entitled to recover reasonable attorneys' fees and costs.

144. As a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff and the Florida Class are entitled to the injunctive relief set forth in the Prayer for Relief set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class

Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining Plaintiff's and Class Members' personally identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks; xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's

final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: August 12, 2022

Respectfully submitted,

/s/ CALEB MARKER

CALEB MARKER (MI Bar #P70963)
ZIMMERMAN REED LLP
6420 Wilshire Blvd. Suite 1080
Los Angeles, CA 90048
Caleb.Marker@zimmreed.com
Telephone: 877.500.8780
Facsimile: 877.500.8781

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW
ANTHONY L. PARKHILL
RILEY W. PRINCE
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: 312.621.2000
Facsimile: 312.641.5504

BARRACK, RODOS & BACINE
STEPHEN R. BASSER*
SAMUEL M. WARD*
600 West Broadway, Suite 900

San Diego, CA 92101
sbasser@barrack.com
sward@barrack.com
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

EMERSON FIRM, PLLC
JOHN EMERSON*
2500 Wilcrest, Suite 300
Houston, TX 77042
Phone: 800-551-8649
Fax: 501-286-4659

Counsel for Plaintiff Rafael Hernandez

* Admission to be sought pursuant to LR 83.20